

Jadavpur University
Department of Computer Science
and Engineering



NETWORKS LAB
ASSIGNMENT 5

BCSE UG-III

Student : Arjeesh Palai
Roll No. : 002310501086
Group : A3
Date : 10 / 11 / 2025

Assignment 5

Task: Packet Tracer & traffic analysis with Wireshark: capture traffic, inspect protocol stacks (Ethernet/IP/TCP/UDP/ICMP/HTTP), use filters, follow streams, view raw bytes, compute latencies, identify NIC OUIs, and generate protocol/flow statistics.

Deliverables: Screenshots and explanations for ICMP/ARP (or ICMPv6 ND), HTTP request/response timing, IP addresses, Host header hex, followed flows, server packet (TCP Src=80) with Ethernet details, NIC manufacturers & OUIs, protocol percentages, and a Flow Graph.

Answers

Q1. ICMP and initial address resolution (ARP / ICMPv6 ND)

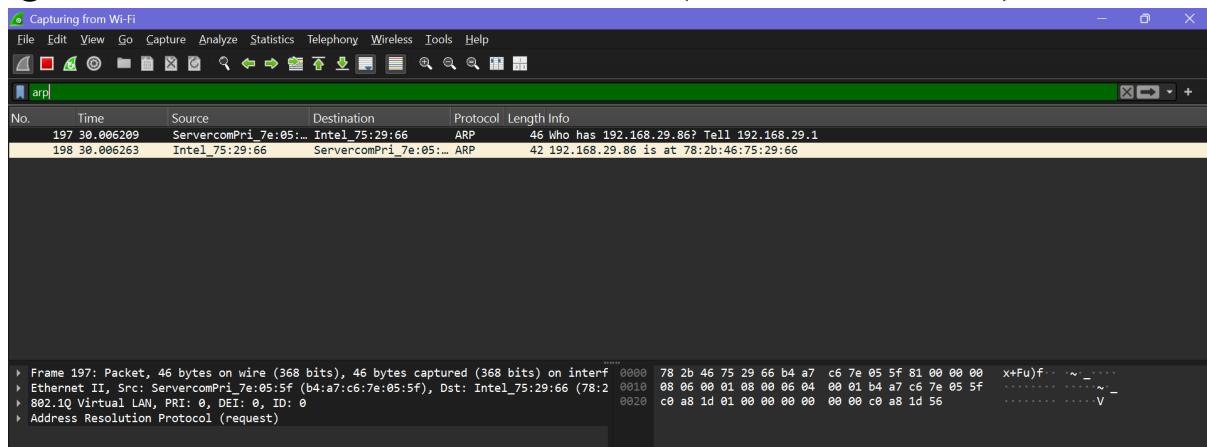


Figure 1: IPv4 ARP request/reply before ICMP echo.

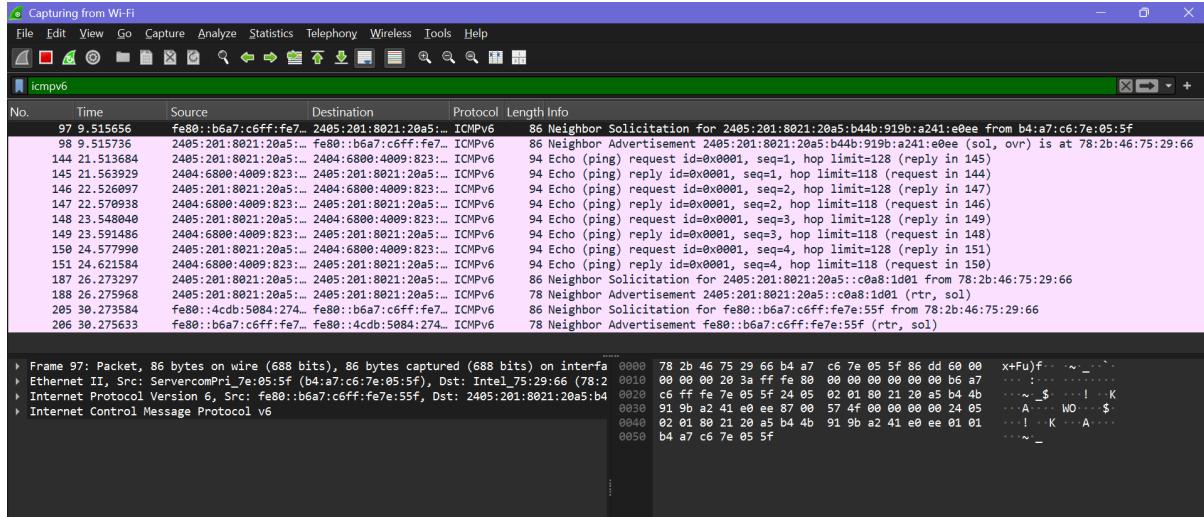


Figure 2: IPv6 Neighbor Solicitation/Advertisement before ICMPv6 echo.

Answer: Started a fresh capture and ran ping. L2 resolution precedes ICMP: ARP (IPv4) or ICMPv6 ND (IPv6). After resolution, Echo Request/Reply pairs appear for the ping exchange.

Q2. Web traffic inspection (protocols, RTT, addresses, Host)

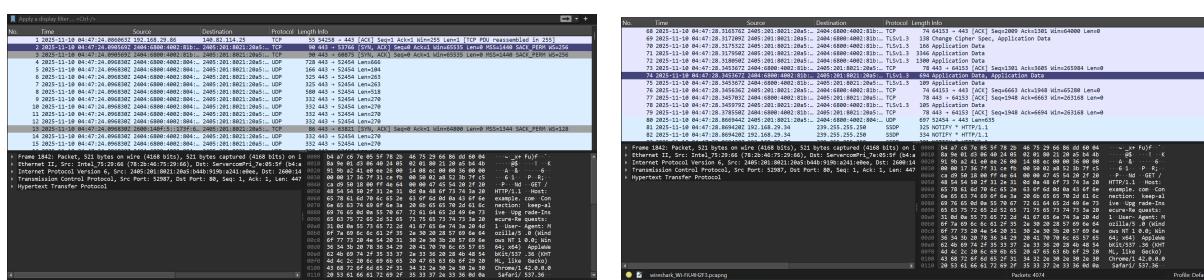


Figure 3: Unfiltered protocol glimpses (1/3).

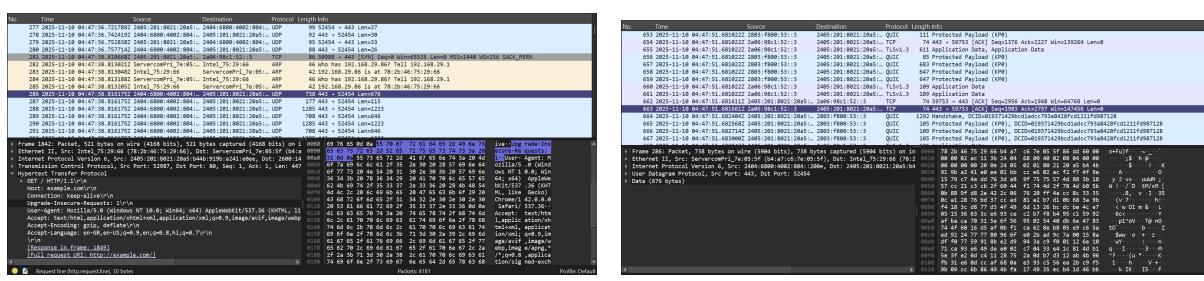


Figure 4: Unfiltered protocol glimpses (2/3).

No.	Time	Source	Destination	Protocol	Length Info
4576	2025-11-10 04:55:44.173233Z	192.168.29.86	35.186.199.248	TCP	54 60970 → 443 [ACK] Seq=2119 Ack=831 Win=64512 Len=0
4577	2025-11-10 04:55:44.252677Z	2405:201:8021:20a5::	2405:201:8021:20a5::	QUIC	1292 Initial, DCID=1621543b507ef13, PKN: 38, PING, PING, PADDING, PING, CRYPTO, CRYPT...
4578	2025-11-10 04:55:44.280531Z	2405:201:8021:20a5::	2405:201:8021:20a5::	DNS	107 Standard query 0x7fcd8 A safetouring.googleapis.com
4579	2025-11-10 04:55:44.284387Z	2405:201:8021:20a5::	2405:201:8021:20a5::	DNS	107 Standard query 0x7fcd8 A safetouring.googleapis.com
4580	2025-11-10 04:55:44.284627Z	2405:201:8021:20a5::	2405:201:8021:20a5::	DNS	107 Standard query 0x7fcd8 A safetouring.googleapis.com
4581	2025-11-10 04:55:44.285932Z	192.168.29.86	1.1.1.1	DNS	85 Standard query 0x7f178 HTTPS chrome.cloudflare-dns.com
4582	2025-11-10 04:55:44.285932Z	192.168.29.86	1.1.1.1	DNS	85 Standard query 0x7f441 AAAA chrome.cloudflare-dns.com
4583	2025-11-10 04:55:44.285961Z	192.168.29.86	1.1.1.1	DNS	117 Standard query response 0xe67f A chrome.cloudflare-dns.com A 172.64.41.3 A 162.15...
4584	2025-11-10 04:55:44.291985Z	192.168.29.86	1.1.1.1	DNS	141 Standard query response 0x7441 AAAA chrome.cloudflare-dns.com AAAA 2803:f808:53::...
4585	2025-11-10 04:55:44.292986Z	192.168.29.86	1.1.1.1	DNS	158 Standard query response 0x9178 HTTPS chrome.cloudflare-dns.com HTTPS
4586	2025-11-10 04:55:44.294140Z	2405:201:8021:20a5::	2405:201:8021:20a5::	QUIC	1292 Initial, DCID=f2b56b3d9d49842f, PKN: 1, PADDING, CRYPTO, CRYPTO, PADDING, PING, C...
4588	2025-11-10 04:55:44.294779Z	2405:201:8021:20a5::	2405:201:8021:20a5::	QUIC	1292 Initial, DCID=f2b56b3d9d49842f, PKN: 2, PING, CRYPTO, CRYPTO, PADDING, CRYPTO, CR...
4589	2025-11-10 04:55:44.294580Z	2405:201:8021:20a5::	2405:201:8021:20a5::	QUIC	139 0-RTT, DCID=f2b56b3d9d49842f
4590	2025-11-10 04:55:44.339473Z	2405:201:8021:20a5::	2405:201:8021:20a5::	QUIC	1292 Initial, DCID=f2b56b3d9d49842f, PKN: 5, PADDING, CRYPTO, PADDING, PING, PING, CRY...
>	Frame 666: Packet, 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0000:b4:a7:c6:7e:05	7f:2b:46:75:29:66	00:00:00:00:00:00		↔ ~_x+Fu)f`...
>	Ethernet II, Src: Intel_75:29:66 (78:2b:46:75:29:66), Dst: ServercomPri_7e:05:5f (b4:a7:c6:7e:05:5f)	00:00:00:00:00:00	00:00:00:00:00:00		7 @S ...K
>	Internet Protocol Version 6, Src: 2405:201:8021:20a5:5b44b:919b:a241:e0ee, Dst: 2803:f808:53::	00:00:00:00:00:00	00:00:00:00:00:00		A <...S
>	User Datagram Protocol, Src Port: 55753, Dst Port: 443	00:00:00:00:00:00	00:00:00:00:00:00		7 -D
>	Quic IETF	00:00:00:00:00:00	00:00:00:00:00:00		00:00:00:00:00:00

Figure 5: Unfiltered protocol glimpses (3/3).

No.	Time	Source	Destination	Protocol	Length Info
1842	74.031239	2405:201:8021:20a5::	2600:1408:ec00:36::	HTTP	521 GET / HTTP/1.1
1843	74.531279	2600:1408:ec00:36::	2405:201:8021:20a5::	HTTP	768 HTTP/1.1 200 OK (text/html)
1870	74.436702	2405:201:8021:20a5::	2600:1408:ec00:36::	HTTP	461 GET /favicon.ico HTTP/1.1
1895	75.048155	2600:1408:ec00:36::	2405:201:8021:20a5::	HTTP	978 HTTP/1.1 404 Not Found (text/html)

Figure 6: HTTP GET packet used for latency measurement.

No.	Time	Source	Destination	Protocol	Length Info
1842	2025-11-10 04:48:38.117302Z	2405:201:8021:20a5::	2600:1408:ec00:36::	HTTP	521 GET / HTTP/1.1
1843	74.031239	2405:201:8021:20a5::	2600:1408:ec00:36::	HTTP	768 HTTP/1.1 200 OK (text/html)
1870	74.436702	2405:201:8021:20a5::	2600:1408:ec00:36::	HTTP	461 GET /favicon.ico HTTP/1.1
1895	75.048155	2600:1408:ec00:36::	2405:201:8021:20a5::	HTTP	978 HTTP/1.1 404 Not Found (text/html)
>	Frame 1842: Packet, 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface 0000:b4:a7:c6:7e:05	05:7f:2b:46:75:29	66:8d:60:00:00:00		↔ ~_x+Fu)f`...
>	Ethernet II, Src: Intel_75:29:66 (78:2b:46:75:29:66), Dst: ServercomPri_7e:05:5f (b4:a7:c6:7e:05:5f)	00:00:00:00:00:00	00:00:00:00:00:00		7 @S ...K
>	Internet Protocol Version 6, Src: 2405:201:8021:20a5:5b44b:919b:a241:e0ee, Dst: 2600:1408:ec00:36::	00:00:00:00:00:00	00:00:00:00:00:00		A & ...6..
>	Transmission Control Protocol, Src Port: 52987, Dst Port: 80, Seq: 1, Ack: 1, Len: 47	00:00:00:00:00:00	00:00:00:00:00:00		6 1 P R...
>	Hypertext Transfer Protocol	00:00:00:00:00:00	00:00:00:00:00:00		P -Nd GET /
>	HTTP/1.1 Host: example.com	00:00:00:00:00:00	00:00:00:00:00:00		example.com
>	HTTP/1.1 Connection: keep-alive	00:00:00:00:00:00	00:00:00:00:00:00		Connection:keep-alive
>	HTTP/1.1 Content-Type: text/html	00:00:00:00:00:00	00:00:00:00:00:00		Content-Type:text/html
>	HTTP/1.1 Date: Mon, 10 Nov 2025 04:48:38 GMT	00:00:00:00:00:00	00:00:00:00:00:00		Date:Mon, 10 Nov 2025 04:48:38 GMT
>	HTTP/1.1 Server: Apache/2.4.42 (Ubuntu)	00:00:00:00:00:00	00:00:00:00:00:00		Server:Apache/2.4.42 (Ubuntu)
>	HTTP/1.1 Last-Modified: Mon, 10 Nov 2025 04:48:38 GMT	00:00:00:00:00:00	00:00:00:00:00:00		Last-Modified:Mon, 10 Nov 2025 04:48:38 GMT
>	HTTP/1.1 Content-Length: 1024	00:00:00:00:00:00	00:00:00:00:00:00		Content-Length:1024
>	HTTP/1.1 Content-Type: text/html; charset=UTF-8	00:00:00:00:00:00	00:00:00:00:00:00		Content-Type:text/html; charset=UTF-8
>	HTTP/1.1 Vary: Accept-Encoding	00:00:00:00:00:00	00:00:00:00:00:00		Vary:Accept-Encoding
>	HTTP/1.1 Pragma: no-cache	00:00:00:00:00:00	00:00:00:00:00:00		Pragma:no-cache
>	HTTP/1.1 Cache-Control: private	00:00:00:00:00:00	00:00:00:00:00:00		Cache-Control:private
>	HTTP/1.1 Age: 0	00:00:00:00:00:00	00:00:00:00:00:00		Age:0
>	HTTP/1.1 Expect: 100-continue	00:00:00:00:00:00	00:00:00:00:00:00		Expect:100-continue
>	HTTP/1.1 Date: Mon, 10 Nov 2025 04:48:38 GMT	00:00:00:00:00:00	00:00:00:00:00:00		Date:Mon, 10 Nov 2025 04:48:38 GMT
>	HTTP/1.1 Content-Type: text/html; charset=UTF-8	00:00:00:00:00:00	00:00:00:00:00:00		Content-Type:text/html; charset=UTF-8
>	HTTP/1.1 Vary: Accept-Encoding	00:00:00:00:00:00	00:00:00:00:00:00		Vary:Accept-Encoding
>	HTTP/1.1 Pragma: no-cache	00:00:00:00:00:00	00:00:00:00:00:00		Pragma:no-cache
>	HTTP/1.1 Cache-Control: private	00:00:00:00:00:00	00:00:00:00:00:00		Cache-Control:private
>	HTTP/1.1 Age: 0	00:00:00:00:00:00	00:00:00:00:00:00		Age:0
>	HTTP/1.1 Expect: 100-continue	00:00:00:00:00:00	00:00:00:00:00:00		Expect:100-continue
>	HTTP/1.1 Date: Mon, 10 Nov 2025 04:48:38 GMT	00:00:00:00:00:00	00:00:00:00:00:00		Date:Mon, 10 Nov 2025 04:48:38 GMT
>	HTTP/1.1 Content-Type: text/html; charset=UTF-8	00:00:00:00:00:00	00:00:00:00:00:00		Content-Type:text/html; charset=UTF-8
>	HTTP/1.1 Vary: Accept-Encoding	00:00:00:00:00:00	00:00:00:00:00:00		Vary:Accept-Encoding
>	HTTP/1.1 Pragma: no-cache	00:00:00:00:00:00	00:00:00:00:00:00		Pragma:no-cache
>	HTTP/1.1 Cache-Control: private	00:00:00:00:00:00	00:00:00:00:00:00		Cache-Control:private
>	HTTP/1.1 Age: 0	00:00:00:00:00:00	00:00:00:00:00:00		Age:0
>	HTTP/1.1 Expect: 100-continue	00:00:00:00:00:00	00:00:00:00:00:00		Expect:100-continue
>	HTTP/1.1 Date: Mon, 10 Nov 2025 04:48:38 GMT	00:00:00:00:00:00	00:00:00:00:00:00		Date:Mon, 10 Nov 2025 04:48:38 GMT
>	HTTP/1.1 Content-Type: text/html; charset=UTF-8	00:00:00:00:00:00	00:00:00:00:00:00		Content-Type:text/html; charset=UTF-8
>	HTTP/1.1 Vary: Accept-Encoding	00:00:00:00:00:00	00:00:00:00:00:00		Vary:Accept-Encoding
>	HTTP/1.1 Pragma: no-cache	00:00:00:00:00:00	00:00:00:00:00:00		Pragma:no-cache
>	HTTP/1.1 Cache-Control: private	00:00:00:00:00:00	00:00:00:00:00:00		Cache-Control:private
>	HTTP/1.1 Age: 0	00:00:00:00:00:00	00:00:00:00:00:00		Age:0
>	HTTP/1.1 Expect: 100-continue	00:00:00:00:00:00	00:00:00:00:00:00		Expect:100-continue
>	HTTP/1.1 Date: Mon, 10 Nov 2025 04:48:38 GMT	00:00:00:00:00:00	00:00:00:00:00:00		Date:Mon, 10 Nov 2025 04:48:38 GMT
>	HTTP/1.1 Content-Type: text/html; charset=UTF-8	00:00:00:00:00:00	00:00:00:00:00:00		Content-Type:text/html; charset=UTF-8
>	HTTP/1.1 Vary: Accept-Encoding	00:00:00:00:00:00	00:00:00:00:00:00		Vary:Accept-Encoding
>	HTTP/1.1 Pragma: no-cache	00:00:00:00:00:00	00:00:00:00:00:00		Pragma:no-cache
>	HTTP/1.1 Cache-Control: private	00:00:00:00:00:00	00:00:00:00:00:00		Cache-Control:private
>	HTTP/1.1 Age: 0	00:00:00:00:00:00	00:00:00:00:00:00		Age:0
>	HTTP/1.1 Expect: 100-continue	00:00:00:00:00:00	00:00:00:00:00:00		Expect:100-continue
>	HTTP/1.1 Date: Mon, 10 Nov 2025 04:48:38 GMT	00:00:00:00:00:00	00:00:00:00:00:00		Date:Mon, 10 Nov 2025 04:48:38 GMT
>	HTTP/1.1 Content-Type: text/html; charset=UTF-8	00:00:00:00:00:00	00:00:00:00:00:00		Content-Type:text/html; charset=UTF-8
>	HTTP/1.1 Vary: Accept-Encoding	00:00:00:00:00:00	00:00:00:00:00:00		Vary:Accept-Encoding
>	HTTP/1.1 Pragma: no-cache	00:00:00:00:00:00	00:00:00:00:00:00		Pragma:no-cache
>	HTTP/1.1 Cache-Control: private	00:00:00:00:00:00	00:00:00:00:00:00		Cache-Control:private
>	HTTP/1.1 Age: 0	00:00:00:00:00:00	00:00:00:00:00:00		Age:0
>	HTTP/1.1 Expect: 100-continue	00:00:00:00:00:00	00:00:00:00:00:00		Expect:100-continue
>	HTTP/1.1 Date: Mon, 10 Nov 2025 04:48:38 GMT	00:00:00:00:00:00	00:00:00:00:00:00		Date:Mon, 10 Nov 2025 04:48:38 GMT
>	HTTP/1.1 Content-Type: text/html; charset=UTF-8	00:00:00:00:00:00	00:00:00:00:00:00		Content-Type:text/html; charset=UTF-8
>	HTTP/1.1 Vary: Accept-Encoding	00:00:00:00:00:00	00:00:00:00:00:00		Vary:Accept-Encoding
>	HTTP/1.1 Pragma: no-cache	00:00:00:00:00:00	00:00:00:00:00:00		Pragma:no-cache
>	HTTP/1.1 Cache-Control: private	00:00:00:00:00:00	00:00:00:00:00:00		Cache-Control:private
>	HTTP/1.1 Age: 0	00:00:00:00:00:00	00:00:00:00:00:00		Age:0
>	HTTP/1.1 Expect: 100-continue	00:00:00:00:00:00	00:00:00:00:00:00		Expect:100-continue
>	HTTP/1.1 Date: Mon, 10 Nov 2025 04:48:38 GMT	00:00:00:00:00:00	00:00:00:00:00:00		Date:Mon, 10 Nov 2025 04:48:38 GMT
>	HTTP/1.1 Content-Type: text/html; charset=UTF-8	00:00:00:00:00:00	00:00:00:00:00:00		Content-Type:text/html; charset=UTF-8
>	HTTP/1.1 Vary: Accept-Encoding	00:00:00:00:00:00	00:00:00:00:00:00		Vary:Accept-Encoding
>	HTTP/1.1 Pragma: no-cache	00:00:00:00:00:00	00:00:00:00:00:00		Pragma:no-cache
>	HTTP/1.1 Cache-Control: private	00:00:00:00:00:00	00:00:00:00:00:00		Cache-Control:private
>	HTTP/1.1 Age: 0	00:00:00:00:00:00	00:00:00:00:00:00		Age:0
>	HTTP/1.1 Expect: 100-continue	00:00:00:00:00:00	00:00:00:00:00:00		Expect:100-continue
>	HTTP/1.1 Date: Mon, 10 Nov 2025 04:48:38 GMT	00:00:00:00:00:00	00:00:00:00:00:00		Date:Mon, 10 Nov 2025 04:48:38 GMT
>	HTTP/1.1 Content-Type: text/html; charset=UTF-8	00:00:00:00:00:00	00:00:00:00:00:00		Content-Type:text/html; charset=UTF-8
>	HTTP/1.1 Vary: Accept-Encoding	00:00:00:00:00:00	00:00:00:00:00:00		Vary:Accept-Encoding
>	HTTP/1.1 Pragma: no-cache	00:00:00:00:00:00	00:00:00:00:00:00		Pragma:no-cache
>	HTTP/1.1 Cache-Control: private	00:00:00:00:00:00	00:00:00:00:00:00		Cache-Control:private
>	HTTP/1.1 Age: 0	00:00:00:00:00:00	00:00:00:00:00:00		Age:0
>	HTTP/1.1 Expect: 100-continue	00:00:00:00:00:00	00:00:00:00:00:00		Expect:100-continue
>	HTTP/1.1 Date: Mon, 10 Nov 2025 04:48:38 GMT	00:00:00:00:00:00	00:00:00:00:00:00		Date:Mon, 10 Nov 2025 04:48:38 GMT
>	HTTP/1.1 Content-Type: text/html; charset=UTF-8	00:00:00:00:00:00	00		

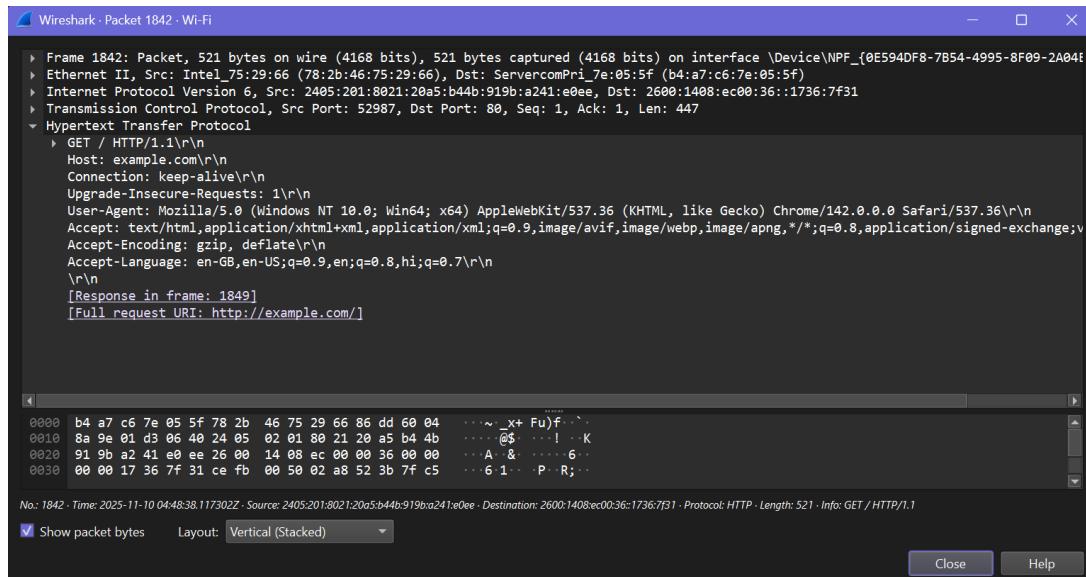


Figure 8: Source/Destination IPs from the GET packet.

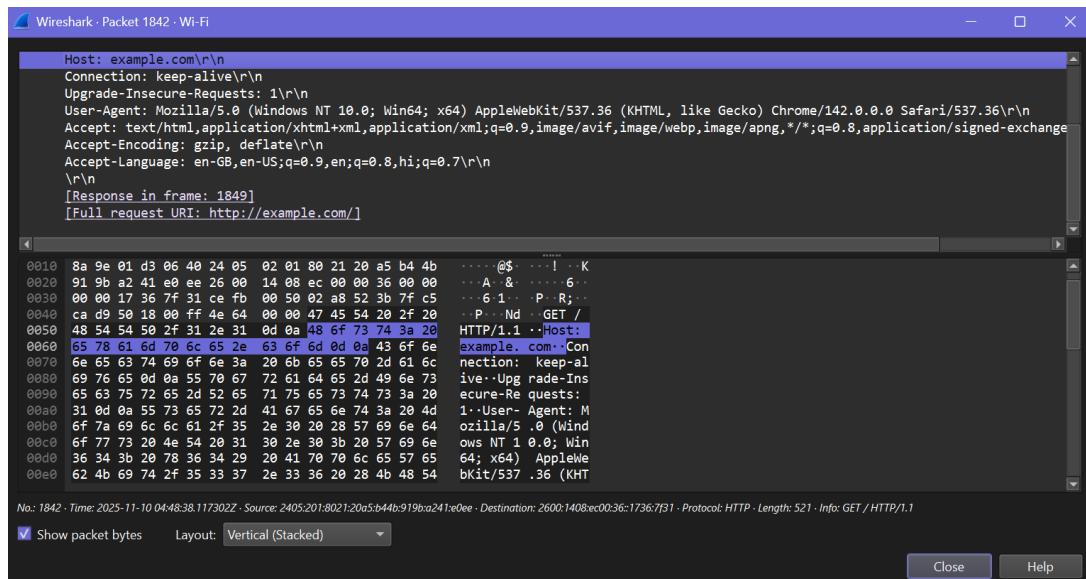


Figure 9: Packet Bytes and HTTP header showing Host:.

- (a) Protocols:** TCP, UDP, HTTP, ARP, DNS, TLS 1.2/1.3, QUIC, SSDP, ICMPv6.
- (b) HTTP latency:** GET at $t = 74.031239$ s; 200 OK at $t = 74.331279$ s $\Rightarrow \Delta t = 0.30004$ s.
- (c) IPs:** Source (host) 2405:201:8021:20a5:b44b:919b:a241:e0ee; Destination (site) 2600:1408:ec00:36:1736:7f31.
- (d/e) Host:** Host: example.com in the HTTP layer.

Q3. Hex and ASCII in Packet Bytes

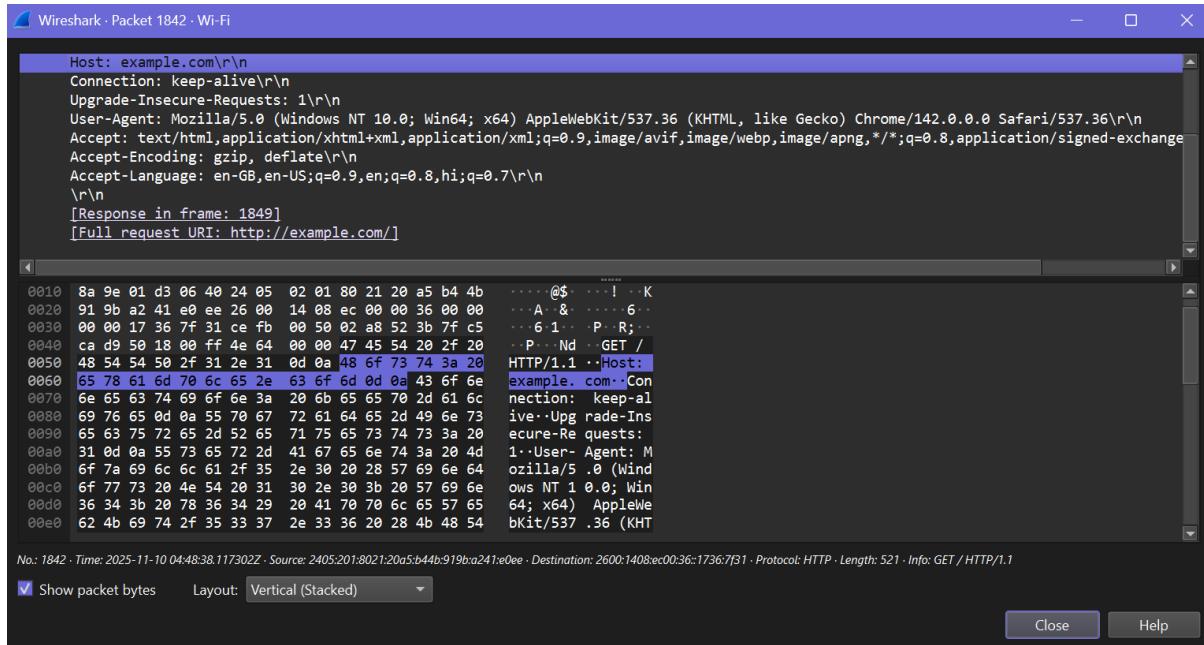
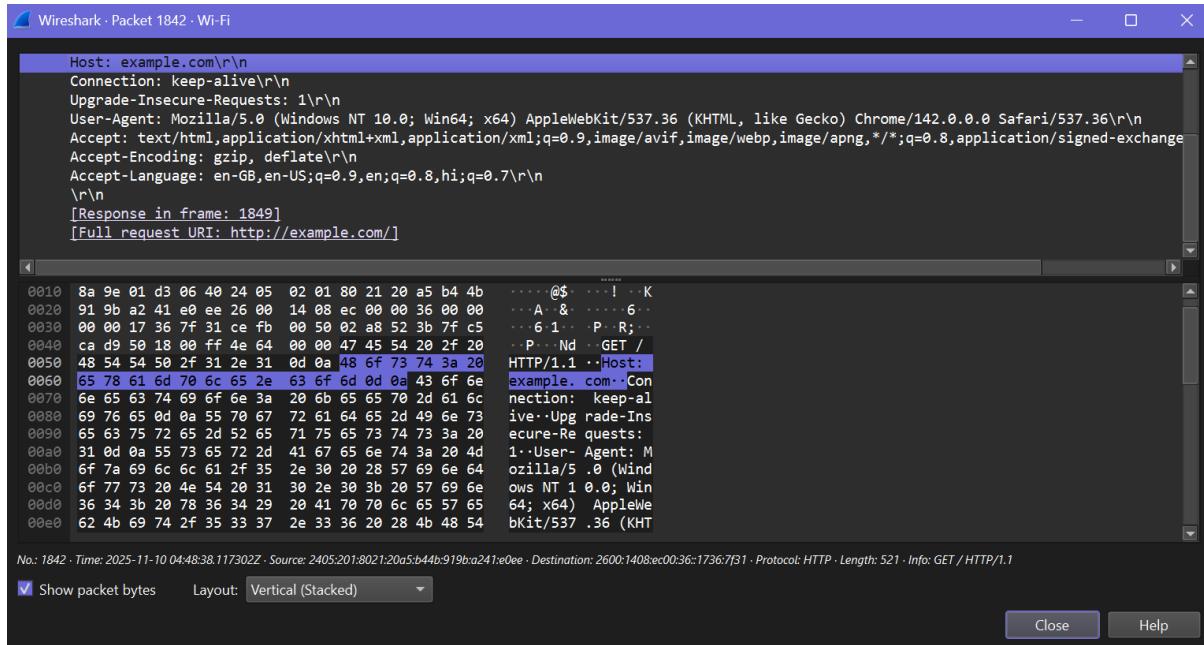


Figure 10: Packet Bytes pane showing aligned Hex and ASCII.

Answer: The lower pane displays offset, hex bytes, and ASCII; the Host: example.com substring is visible with matching hex.

Q4. First 4 bytes of Hex for the Host value

Figure 11: Locating the start of `example.com` for hex extraction.

Answer: The first four bytes of the value (*exam*) are **65 78 61 6d**.

Q5. Follow a conversation (flow)

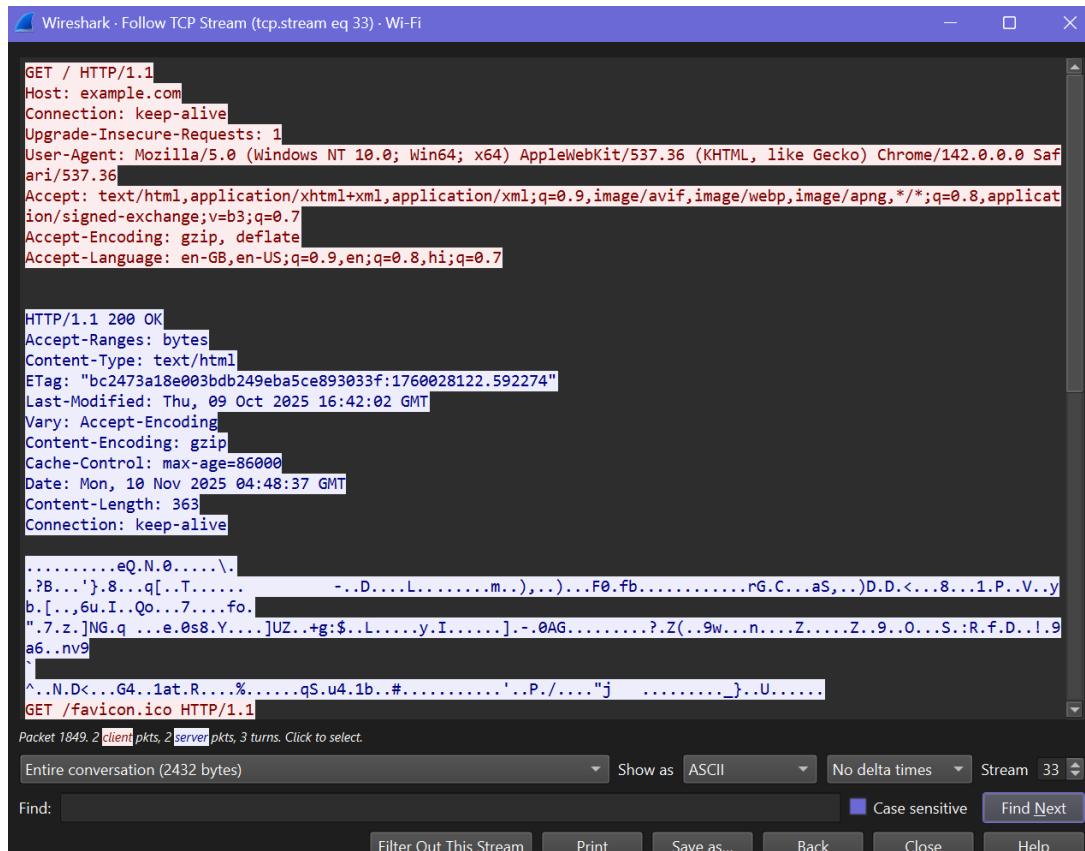


Figure 12: Follow → TCP Stream: reassembled request.

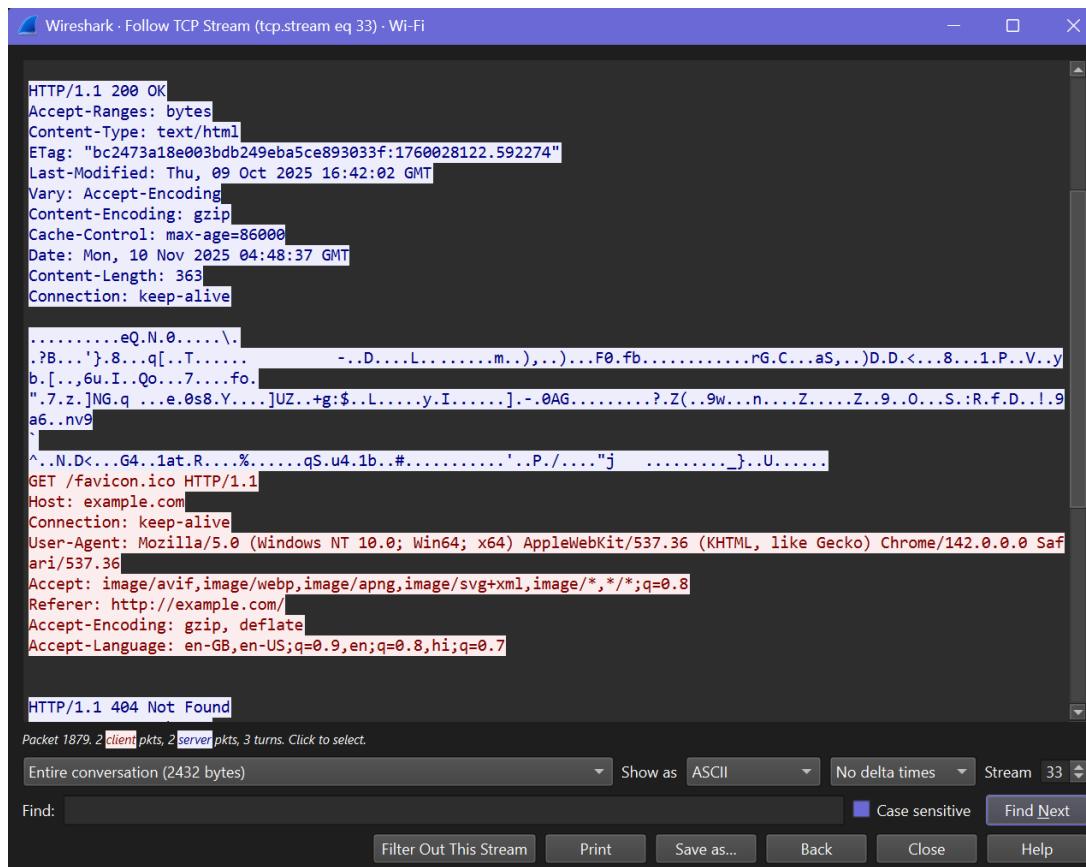


Figure 13: Follow → TCP Stream: reassembled response.

Answer: Using Follow TCP Stream reconstructs the HTTP GET and the subsequent 200 OK with payload.

Q6. HTTP packet from server (TCP Source Port = 80)

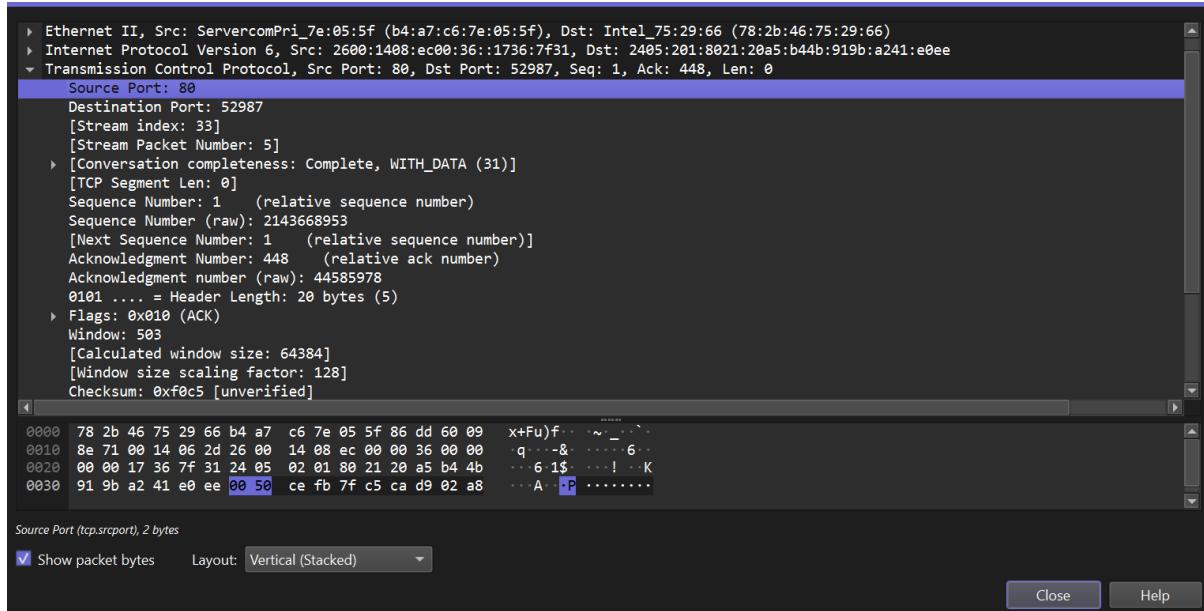


Figure 14: Server → client segment with TCP Src=80 and Ethernet expanded.

Answer: A server-to-client HTTP packet shows TCP Source Port = 80; expanding Ethernet reveals MAC addressing.

Q7. NIC manufacturers (vendor resolution)

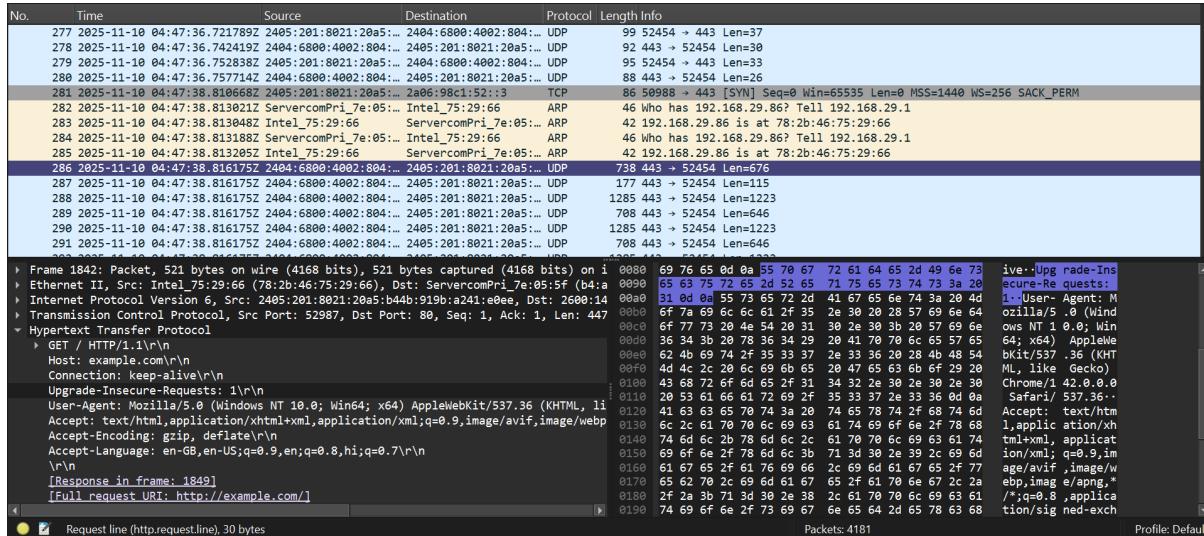


Figure 15: Ethernet II details with vendor names (name resolution enabled).

Answer: Vendor mapping indicates the host NIC as **Intel** and the server NIC as **ServercomPri** (example frames shown).

Q8. Hex OUIs (first three bytes of each MAC)

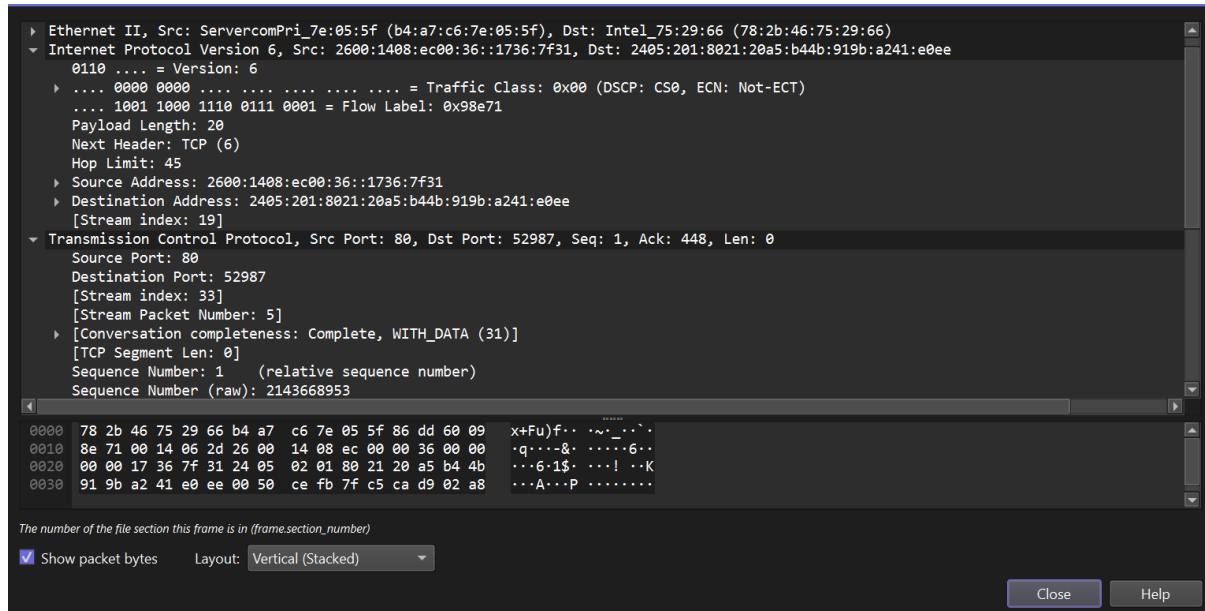


Figure 16: Reading OUIs (first 3 bytes) from MAC addresses.

Answer: OUIs observed: Intel **78 : 2b : 46**; ServercomPri **b4 : a7 : c6**.

Q9. Protocol percentages (TCP vs UDP)

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	3627	100.0	1169618	8279	0	0	0	3627
Ethernet	100.0	3627	4.3	50802	359	0	0	0	3627
Internet Protocol Version 6	45.5	1649	5.6	65960	466	0	0	0	1649
Transmission Control Protocol	45.5	1649	3.1	35932	254	960	22152	156	1649
Transport Layer Security	18.1	657	33.5	392034	2775	657	356575	2524	677
Hypertext Transfer Protocol	0.1	4	0.1	1556	11	2	834	5	4
Line-based text data	0.1	2	0.1	1026	7	2	1026	7	2
Data	0.8	28	0.0	28	0	28	28	0	28
Internet Protocol Version 4	45.4	1646	2.8	32920	233	0	0	0	1646
Transmission Control Protocol	45.4	1646	3.1	36480	258	1138	26320	186	1646
Transport Layer Security	13.5	490	32.8	384162	2719	490	357163	2528	503
Data	0.5	18	0.0	18	0	18	18	0	18
802.1Q Virtual LAN	9.2	333	0.1	1332	9	0	0	0	333
Internet Protocol Version 6	9.2	332	1.1	13280	94	0	0	0	332
Transmission Control Protocol	9.2	332	0.6	7060	49	211	4640	32	332
Transport Layer Security	3.3	121	5.1	59164	418	121	44512	315	133

Figure 17: Protocol Hierarchy (*capture must be unfiltered*).

Answer: Clear display filters → **Statistics** → **Protocol Hierarchy** to obtain accurate TCP/UDP percentages for the entire capture.

Q10. Flow Graph



Figure 18: Statistics → Flow Graph summarizing per-flow timelines.

Answer: The graph shows SYN/SYN-ACK/ACK transitions and request/response ordering across concurrent connections.

Appendix: Capture Steps

- Selected the correct NIC and started capture.
- Enabled MAC name resolution for vendor IDs.
- Generated traffic: ping, web browsing (HTTP/HTTPS), DNS lookups.
- Used filters (`http`, `tcp`, `dns`), Follow Streams, Protocol Hierarchy, and Flow Graph.